

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-069597

(43)Date of publication of application : 07.03.2003

(51)Int.Cl.

H04L 12/46

H04L 9/08

H04L 12/66

(21)Application number : 2001-257681

(71)Applicant : NEC CORP

(22)Date of filing : 28.08.2001

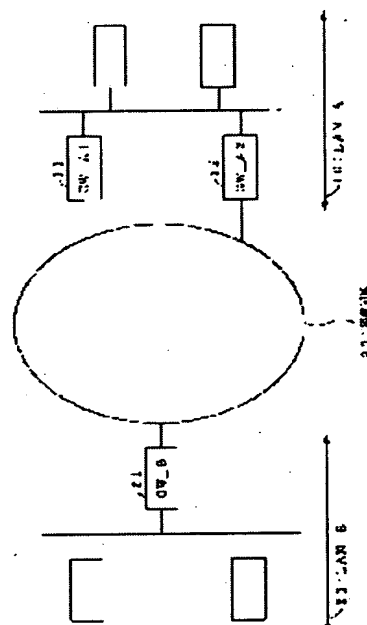
(72)Inventor : YAMAGUCHI TAKAHIRO

(54) LARGE-SCALE IPSec VPN CONSTRUCTION METHOD, LARGE-SCALE IPSec VPN SYSTEM AND PROGRAM, AND KEY SHARING INFORMATION PROCESSING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To enable IPSec (Security architecture for IP) communication using a key even if a fault occurs in a gateway where a key exchange is performed, in a large-scale LAN having a plurality of gateways.

SOLUTION: When the key exchange based on IPSec is performed between the gateway of the large-scale LAN having a plurality of gateways and a gateway of another LAN, an Internet key exchange portion in the gateway of the large-scale LAN sets a key in an IPSec portion of this gateway, and requests a key transferring portion of this gateway to transfer the key. In response to this request, the key transferring portion transfers the key to a key transferring portion of another gateway in the large-scale LAN, and the key transferring portion of the other gateway sets the key in an IPSec portion of the other gateway by using this transferred key.



LEGAL STATUS

[Date of request for examination]

19.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3651424

[Date of registration]

04.03.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-69597

(P2003-69597A)

(43)公開日 平成15年3月7日(2003.3.7)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-ト [*] (参考)
H 0 4 L 12/46	1 0 0	H 0 4 L 12/46	V 5 J 1 0 4
9/08		12/66	1 0 0 R 5 K 0 3 0
12/66		9/00	B 5 K 0 3 3
			6 0 1 C
			6 0 1 E
審査請求 有 請求項の数13 OL (全 12 頁)			

(21)出願番号 特願2001-257681(P2001-257681)

(22)出願日 平成13年8月28日(2001.8.28)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 山口 恭弘

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100086759

弁理士 渡辺 喜平

Fターム(参考) 5J104 AA16 EA02 EA04 EA16 JA03
NA02 PA07

5K030 CA11 HA08 HC14 HD03 LD19

5K033 AA04 CB01 CC01 DA01 DA05

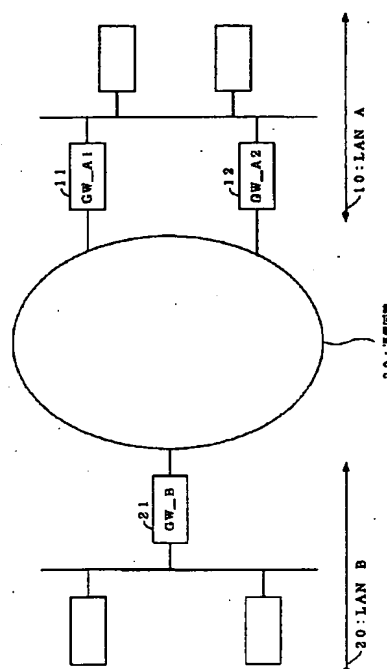
DB19 EA03

(54)【発明の名称】 大規模IPSecVPN構築方法、大規模IPSecVPNシステム、プログラム及び鍵共有情報処理装置

(57)【要約】

【課題】 複数のゲートウェイを有する大規模LANにおいて、鍵交換を行ったゲートウェイに障害が発生しても、その鍵を使ったIPSec通信を可能とする。

【解決手段】 複数のゲートウェイを有する大規模LANのゲートウェイと、その他のLANのゲートウェイとの間で、IPSecにもとづく鍵交換が行われた場合において、大規模LANのゲートウェイのインターネットキーエクスチェンジ部が、このゲートウェイのIPSec部に鍵設定を行うとともに、このゲートウェイの鍵転送部に鍵転送を要求し、この要求に応じて鍵転送部が、大規模LANの他のゲートウェイの鍵転送部に鍵転送を行い、他のゲートウェイの鍵転送部が、この転送されてきた鍵を用いて、他のゲートウェイのIPSec部に鍵設定を行う。



【特許請求の範囲】

【請求項1】 複数のゲートウェイを有する大規模LANのゲートウェイと、その他のLANのゲートウェイとの間で、IPSecにもとづく鍵交換が行われた場合において、

前記大規模LANのゲートウェイのインターネットキーエクスチェンジ部が、このゲートウェイのIPSec部に鍵設定を行うとともに、このゲートウェイの鍵転送部に鍵転送を要求し、

前記ゲートウェイの鍵転送部が、前記要求に応じて、前記大規模LANの他のゲートウェイの鍵転送部に鍵転送を行い、

前記他のゲートウェイの鍵転送部が、この転送されてきた鍵を用いて、前記他のゲートウェイのIPSec部に鍵設定を行うことを特徴とする大規模IPSec VPNの構築方法。

【請求項2】 前記鍵転送は、

前記大規模LANの前記ゲートウェイが、前記大規模LANの前記他のゲートウェイに鍵転送を要求し、

前記他のゲートウェイが、この要求に対して、OK信号を暗号化して前記ゲートウェイに返し、

前記ゲートウェイが、この暗号化されたOK信号を検査するとともに、前記鍵を暗号化して前記他のゲートウェイに転送し、

前記他のゲートウェイが、この転送されてきた鍵を検査して、前記ゲートウェイにOK信号を返す手順を含むことを特徴とする請求項1記載の大規模IPSec VPNの構築方法。

【請求項3】 前記大規模LANの前記他のゲートウェイの鍵転送部が、前記大規模LANの前記ゲートウェイから鍵転送を受けると、前記他のゲートウェイのIPSec部に鍵設定を行うとともに、この鍵を前記大規模LANのさらなる他のゲートウェイの鍵転送部に転送し、前記さらなる他のゲートウェイも、前記他のゲートウェイと同様に、自分のIPSec部に鍵設定を行うとともに、この鍵を前記ゲートウェイの鍵転送部に転送し、前記ゲートウェイは、転送されてきた前記鍵が、最初に自分が転送した鍵に一致することを確認することを特徴とする請求項1又は2記載の大規模IPSec VPNの構築方法。

【請求項4】 複数のゲートウェイを有する大規模LANのゲートウェイと、その他のLANのゲートウェイとの間で、IPSecにもとづく鍵交換が行われると、前記大規模LAN内のゲートウェイ間で鍵転送が行われる大規模IPSec VPNシステムであって、

インターネットキーエクスチェンジ部により前記その他のLANのゲートウェイと鍵交換を行うとともに、このインターネットキーエクスチェンジ部により自分のIPSec部に鍵設定を行って、自分の鍵転送部に鍵転送を要求し、この鍵転送部により前記大規模LANの他のゲ

ートウェイに鍵転送を行う前記大規模LANの前記ゲートウェイと、

前記大規模LANの前記ゲートウェイから、鍵転送部が鍵転送を受けるとともに、自分のIPSec部に鍵設定を行う前記大規模LANの前記他のゲートウェイと、

前記大規模LANの前記ゲートウェイと鍵交換を行う前記その他のLANのゲートウェイと、

前記大規模LANの前記ゲートウェイと、前記大規模LANの前記他のゲートウェイと、前記その他のLANのゲートウェイを接続する通信回線とを有することを特徴とする大規模IPSec VPNシステム。

【請求項5】 前記鍵転送は、

前記大規模LANの前記ゲートウェイが、前記大規模LANの前記他のゲートウェイに鍵転送を要求し、

前記他のゲートウェイが、この要求に対して、OK信号を暗号化して前記ゲートウェイに返し、

前記ゲートウェイが、この暗号化されたOK信号を検査するとともに、前記鍵を暗号化して前記他のゲートウェイに転送し、

前記他のゲートウェイが、この転送されてきた鍵を検査して、前記ゲートウェイにOK信号を返す手順を含むことを特徴とする請求項4記載の大規模IPSec VPNシステム。

【請求項6】 前記大規模LANの前記他のゲートウェイの鍵転送部が、前記大規模LANの前記ゲートウェイから鍵転送を受けると、前記他のゲートウェイのIPSec部に鍵設定を行うとともに、この鍵を前記大規模LANのさらなる他のゲートウェイの鍵転送部に転送し、前記さらなる他のゲートウェイも、前記他のゲートウェイと同様に、自分のIPSec部に鍵設定を行うとともに、この鍵を前記ゲートウェイの鍵転送部に転送し、前記ゲートウェイは、転送されてきた前記鍵が、最初に自分が転送した鍵に一致することを確認することを特徴とする請求項4又は5記載の大規模IPSec VPNシステム。

【請求項7】 前記転送が、前記大規模LANが有する4台以上のゲートウェイについて同様に行われることを特徴とする請求項6記載の大規模IPSec VPNシステム。

【請求項8】 前記大規模LANの前記ゲートウェイと、前記その他のLANのゲートウェイが鍵交換を行うとともに、前記大規模LANの前記ゲートウェイが、前記大規模LANの前記他のゲートウェイに鍵転送を行い、

前記大規模LANの前記ゲートウェイに障害が発生すると、

通信回線上の複数のルータの情報交換によって、前記大規模LANの前記ゲートウェイ宛の転送を、前記大規模LANの前記他のゲートウェイに対して行うように経路情報が修正され、

【0005】

【発明が解決しようとする課題】しかしながら、このような従来の方法などは、ゲートウェイの障害に備えて、常にその動作状況を監視する必要があることに加え、障害が発生した場合には、別のゲートウェイと再度新たに鍵の共有を行う必要があり、ネットワークに高い負荷をかける方法であった。このため、一つのゲートウェイで障害が発生しても別のゲートウェイを経由してLAN外との通信を行うことのできる大規模LANの利点を損なうことなく、IPSecによるセキュリティの確保を可能とする方法等の実現が望まれていた。

【0006】本発明は、上記の事情にかんがみなされたものであり、従来のようなIPSecにおける不都合を解消し、IPSecによるセキュリティの確保されたゲートウェイにおいて障害が発生しても、ネットワークに高負荷をかけることなく、別のゲートウェイを経由して、LAN外からの通信を可能とする大規模IPSec VPN (Virtual Private Network) 構築方法、大規模IPSec VPNシステム、大規模IPSec VPNプログラム及び鍵共有情報処理装置の提供を目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、本発明の請求項1記載の大規模IPSec VPNの構築方法は、複数のゲートウェイを有する大規模LANのゲートウェイと、その他のLANのゲートウェイとの間で、IPSecにもとづく鍵交換が行われた場合において、大規模LANのゲートウェイのインターネットキーエクスチェンジ部が、このゲートウェイのIPSec部に鍵設定を行うとともに、このゲートウェイの鍵転送部に鍵転送を要求し、ゲートウェイの鍵転送部が、要求に応じて、大規模LANの他のゲートウェイの鍵転送部に鍵転送を行い、他のゲートウェイの鍵転送部が、この転送されてきた鍵を用いて、他のゲートウェイのIPSec部に鍵設定を行う方法としてある。

【0008】大規模IPSec VPNの構築方法をこのような方法にすれば、大規模LAN内において、鍵交換を行ったゲートウェイが、他のゲートウェイにその鍵をコピーし、実際には鍵交換を行っていないゲートウェイに、鍵交換を行った場合と同様の権限をもたせることができる。

【0009】このため、鍵交換を行ったゲートウェイに障害が発生しても、他のゲートウェイが、その障害が発生したゲートウェイに代わり、同様の役割を果たすことが可能となるため、このような場合に通信不能とはならなくなる。また、この方法によれば、余分に鍵交換を行う必要がなくなるため、ネットワークや、ゲートウェイにかかる負荷を大幅に軽減することが可能となる。

【0010】次に、本発明の請求項2記載の大規模IPSec VPNの構築方法は、鍵転送は、大規模LAN

のゲートウェイが、大規模LANの他のゲートウェイに鍵転送を要求し、他のゲートウェイが、この要求に対して、OK信号を暗号化してゲートウェイに返し、ゲートウェイが、この暗号化されたOK信号を検査するとともに、鍵を暗号化して他のゲートウェイに転送し、他のゲートウェイが、この転送されてきた鍵を検査して、ゲートウェイにOK信号を返す手順を含む方法としてある。

【0011】大規模IPSec VPNの構築方法をこのような方法にすれば、鍵転送を行う場合において、セキュリティを確保することが可能となり、この鍵転送を行うLANの内部に悪意のユーザが存在したとしても、盗聴などが行われることを防止することができる。

【0012】次に、本発明の請求項3記載の大規模IPSec VPNの構築方法は、大規模LANの他のゲートウェイの鍵転送部が、大規模LANのゲートウェイから鍵転送を受けると、他のゲートウェイのIPSec部に鍵設定を行うとともに、この鍵を大規模LANのさらなる他のゲートウェイの鍵転送部に転送し、さらなる他のゲートウェイも、他のゲートウェイと同様に、自分のIPSec部に鍵設定を行うとともに、この鍵をゲートウェイの鍵転送部に転送し、ゲートウェイは、転送されてきた鍵が、最初に自分が転送した鍵に一致することを確認する方法としてある。

【0013】大規模IPSec VPNの構築方法をこのような方法にすれば、大規模LANのゲートウェイが、3台以上の場合には、鍵転送を受けたゲートウェイが、さらに他のゲートウェイに鍵転送を行うことができ、鍵転送を効率的に行うことが可能となる。また、大規模LAN内のゲートウェイが多数ある場合には、鍵交換を行ったゲートウェイと鍵転送を受けたゲートウェイをコピー元として、同時に複数の転送を行うことによって、速やかに鍵転送を行うことも可能となる。

【0014】次に、本発明の請求項4記載の大規模IPSec VPNシステムは、複数のゲートウェイを有する大規模LANのゲートウェイと、その他のLANのゲートウェイとの間で、IPSecにもとづく鍵交換が行われると、大規模LAN内のゲートウェイ間で鍵転送が行われる大規模IPSec VPNシステムであって、インターネットキーエクスチェンジ部によりその他のLANのゲートウェイと鍵交換を行うとともに、このインターネットキーエクスチェンジ部により自分のIPSec部に鍵設定を行って、自分の鍵転送部に鍵転送を要求し、この鍵転送部により大規模LANの他のゲートウェイに鍵転送を行う大規模LANのゲートウェイと、大規模LANのゲートウェイから、鍵転送部が鍵転送を受けるとともに、自分のIPSec部に鍵設定を行う大規模LANの他のゲートウェイと、大規模LANのゲートウェイと鍵交換を行うその他のLANのゲートウェイと、大規模LANのゲートウェイと、大規模LANの他のゲートウェイと、その他のLANのゲートウェイを接続す

る通信回線とを有する構成としてある。

【0015】大規模IPSec VPNシステムをこのような構成にすれば、鍵交換を行ったゲートウェイに障害が発生しても、他のゲートウェイが、その障害が発生したゲートウェイに代わり、同様の役割を果たすことが可能となるため、IPSec通信不能とはならなくなる。

【0016】また、従来技術にあるように、別途鍵交換を行うことによって、迂回用のゲートウェイを設定する場合に比べると、本システムでは負荷の大きい鍵交換を1度しか行う必要がないため、ネットワークや、ゲート

ウェイにかかる負荷を大幅に軽減することが可能となる。

【0017】次に、本発明の請求項5記載の大規模IPSec VPNシステムは、鍵転送は、大規模LANのゲートウェイが、大規模LANの他のゲートウェイに鍵転送を要求し、他のゲートウェイが、この要求に対して、OK信号を暗号化してゲートウェイに返し、ゲート

ウェイが、この暗号化されたOK信号を検査するとともに、鍵を暗号化して他のゲートウェイに転送し、他のゲートウェイが、この転送されてきた鍵を検査して、ゲート

ウェイにOK信号を返す手順を含む構成としてある。

【0018】大規模IPSec VPNシステムをこのような構成にすれば、LANの内部に悪意のユーザが存在したとしても、鍵転送時における盗聴などを防止することが可能となる。

【0019】次に、本発明の請求項6記載の大規模IPSec VPNシステムは、大規模LANの他のゲート

ウェイの鍵転送部が、大規模LANのゲートウェイから鍵転送を受けると、他のゲートウェイのIPSec部に

鍵設定を行うとともに、この鍵を大規模LANのさらなる他のゲートウェイの鍵転送部に転送し、さらなる他のゲートウェイも、他のゲートウェイと同様に、自分のIPSec部に鍵設定を行うとともに、この鍵をゲート

ウェイ自体も、他のゲートウェイに対して鍵転送を行うことが可能となる。

【0022】この場合、鍵転送を受けたゲートウェイが、次に他のゲートウェイに鍵転送を順次行うといったように、単に複数の鍵転送を直線的に実施するのみならず、所定の鍵転送経路を設定するなどして、鍵交換を行ったゲートウェイと鍵転送を受けたゲートウェイをコピー元として、複数の転送を同時に実行することによって、速やかに転送を行うことも可能である。

【0023】次に、本発明の請求項8記載の大規模IPSec VPNシステムは、大規模LANのゲートウェイと、その他のLANのゲートウェイが鍵交換を行うとともに、大規模LANのゲートウェイが、大規模LANの他のゲートウェイに鍵転送を行い、大規模LANのゲートウェイに障害が発生すると、通信回線上の複数のルータの情報交換によって、大規模LANのゲートウェイ宛の転送を、大規模LANの他のゲートウェイに対して行うように経路情報が修正され、大規模LANのホストに対して、その他のLANの他のホストからパケット発信がなされると、その他のLANのゲートウェイが、このパケットをカプセル化して、大規模LANのゲート

ウェイ宛に通信回線を介して送信し、送信されたパケットが、修正された経路情報に従って、大規模LANの他のゲートウェイに転送され、大規模LANの他のゲートウェイが、送信されたパケットの逆カプセル化を行って、大規模LANのホストに送信し、大規模LANのホストがこの送信されてきたパケットの受信を行う構成としてある。

【0024】大規模IPSec VPNシステムをこのような構成にすれば、大規模LANにおける鍵交換を行ったゲートウェイに障害が発生しても、鍵交換を行った時点で事前に、大規模LANにおける他のゲートウェイに鍵転送が行われているため、その他のLANの他のホストから、その他のLANにおける上記鍵交換を行ったゲートウェイを経由して、大規模LANのホストに対してパケットが送信された場合に、上記障害が発生したゲートウェイを迂回し、鍵転送を受けた他のゲートウェイを経由して、適切なホストに受信させることが可能となる。なお、この場合のホストとは、所謂ホストコンピュータに限定する意味のものではなく、端末やサーバ等、ネットワークに接続する広く一般の情報処理装置を意味するものである。

【0025】次に、本発明の請求項9記載の大規模IPSec VPNプログラムは、大規模LAN内において、鍵転送を行う大規模IPSec VPNプログラムであって、大規模LANのゲートウェイのインターネットキーエクスチェンジ部が、鍵交換を行った場合には、ゲートウェイのインターネットキーエクスチェンジ部に、ゲートウェイのIPSec部に対して鍵設定を行わせるとともに、ゲートウェイの鍵転送部に対して鍵転送

を要求させ、ゲートウェイの鍵転送部に、大規模LANの他のゲートウェイの鍵転送部に対して鍵転送を行わせ、大規模LANのゲートウェイの鍵転送部が、鍵転送を受けた場合には、この鍵転送部に、転送されてきた鍵を用いて、ゲートウェイのIPSec部に対して鍵設定を行わせる構成としてある。

【0026】大規模IPSec VPNプログラムをこのような構成にすれば、鍵交換を行ったゲートウェイに障害が発生しても、他のゲートウェイにその代役をさせることができるため、このような場合にIPSec通信不能となることを防止することが可能となる。また、従来技術の別途鍵交換を行うことにより迂回用のゲートウェイを設定する場合に比べると、負荷の大きい鍵交換を1度しか行わないため、ネットワークや、ゲートウェイにかかる負荷を大幅に軽減させることが可能となる。

【0027】次に、本発明の請求項10記載の大規模IPSec VPNプログラムは、鍵転送は、大規模LANのゲートウェイに、大規模LANの他のゲートウェイに対して鍵転送を要求させ、他のゲートウェイに、この要求に対して、OK信号を暗号化させてゲートウェイに返却させ、ゲートウェイに、この暗号化されたOK信号を検査させるとともに、鍵を暗号化させて他のゲートウェイに転送させ、他のゲートウェイに、この転送されてきた鍵を検査させて、ゲートウェイにOK信号を返却させる手順を含む構成としてある。

【0028】大規模IPSec VPNプログラムをこのような構成にすれば、LANの内部に悪意のユーザが存在したとしても、鍵転送時における盗聴などを防止させることが可能となる。

【0029】次に、本発明の請求項11記載の大規模IPSec VPNプログラムは、大規模LANのゲートウェイの鍵転送部が、鍵転送を受けた場合には、この転送されてきた鍵を用いて、ゲートウェイの鍵転送部に、ゲートウェイのIPSec部に対して鍵設定を行わせるとともに、大規模LANのさらなる他のゲートウェイに対して鍵転送を行わせる構成としてある。

【0030】大規模IPSec VPNプログラムをこのような構成にすれば、大規模LANのゲートウェイが、3台以上の場合に、鍵転送を受けたゲートウェイに、さらに他のゲートウェイへ鍵転送を行わせることができるため、鍵転送の効率化を図ることが可能となる。

【0031】次に、本発明の請求項12記載の鍵共有情報処理装置は、通信回線を介してIPSecによる鍵交換を行う際に、鍵転送も行う鍵共有情報処理装置であって、鍵共有情報処理装置のインターネットキーエクスチェンジ部が、鍵交換を行った場合には、このインターネットキーエクスチェンジ部が、鍵共有情報処理装置のIPSec部に鍵設定を行うとともに、鍵共有情報処理装置の鍵転送部に鍵転送を要求し、この鍵転送部が他の鍵共有情報処理装置に鍵転送を行い、鍵共有情報処理装置

の鍵転送部が、鍵転送を受けた場合には、この転送されてきた鍵を用いて、鍵共有情報処理装置のIPSec部に鍵設定を行う構成としてある。

【0032】鍵共有情報処理装置をこのような構成にすれば、自分が鍵交換を行った場合には、自身のIPSec部に鍵設定を行うとともに、他の鍵共有情報処理装置に鍵を転送し、他の鍵共有情報処理装置が鍵設定を行った場合には、鍵転送を受けるとともに、この転送されてきた鍵を自身のIPSec部に設定することが可能となる。

【0033】そして、大規模LANなどにおいて、このような鍵共有情報処理装置をLAN外との情報の送受信の窓口として用いることにより、特定の鍵共有情報処理装置に障害が発生しても、この鍵共有情報処理装置から鍵転送を受けた他の鍵共有情報処理装置が、その代役を果たすことにより、通信不能となることを防止することが可能となる。

【0034】また、このような鍵共有情報処理装置を、大規模IPSec VPN以外に適用してもかまわない。例えば、インターネットショッピングなどにおいて、利用者端末が、ショップにおける本発明の鍵共有情報処理装置とセキュリティを確立する際に、ショップの別個の鍵共有情報処理装置に鍵転送を行うことによって、利用者のショッピング中にショップの鍵共有情報処理装置に障害が発生しても、その別個の鍵共有情報処理装置に以降の処理を代行させることによって、通信不能となることを防止することが可能となる。

【0035】次に、本発明の請求項13記載の鍵共有情報処理装置は、大規模IPSec VPNにおけるゲートウェイである構成としてある。鍵共有情報処理装置をこのような構成にすれば、上記のような鍵転送機能を大規模IPSec VPNにおけるゲートウェイにもたせることが可能となる。

【0036】

【発明の実施の形態】以下、本発明の実施形態につき、図面を参照して説明する。

【第一実施形態】まず、本発明の第一実施形態について、図1を参照して説明する。同図は、本実施形態における大規模IPSec VPNシステムの構成を示すブロック図である。

【0037】同図に示すように、大規模IPSec VPNシステムは、LAN A10、LAN B20及び通信回線30を有している。LAN A10は、複数のゲートウェイを有する大規模LANであって、ゲートウェイA1 (GW_A1) 11とゲートウェイA2 (GW_A2) 12等を有している。

【0038】また、LAN B20は、その他のLANであって、その規模に特に制限はないが、ゲートウェイB (GW_B) 21等を有している。これらLAN A10とLAN B20とは通信回線30を介して接続さ

れている。

【0039】そして、これらLAN A10とLAN B20が通信するにあたり、IPSecによるセキュリティを確保したい場合には、通常、例えばゲートウェイA111と、ゲートウェイB21が、IKE（インターネットキーエクスチェンジ）による鍵交換を行って同じ鍵を共有し、その鍵を使ってIPSec通信を行う。

【0040】この際、本実施形態においては、ゲートウェイA111と、ゲートウェイB21が鍵交換を行うにあたり、ゲートウェイA111が、ゲートウェイA212に鍵転送を行って、その後ゲートウェイA111に障害が発生しても、ゲートウェイA212にIPSec通信機能を代行させることを可能とする。

【0041】通信回線30としては、従来公知の任意好適な公衆回線、商業回線又は専用回線を用いることができる。また、ゲートウェイA111、ゲートウェイA212及びゲートウェイB21等のそれぞれの間においては、同一又は別個の通信回線で構成することができる。

【0042】さらに、通信回線30は、ゲートウェイA111、ゲートウェイA212及びゲートウェイB21等のそれぞれの間を、無線あるいは有線で接続可能な回線であり、例えば、携帯端末網、公衆回線網、専用回線網及びインターネット回線網により構成することができる。

【0043】次に、図2を用いて、上記各ゲートウェイの機能について、その処理手順とともに詳細に説明する。ゲートウェイA111は、IKE部111、IPSec部112、鍵転送部113を有している。また、ゲートウェイA212も同様に、IKE部121、IPSec部122、鍵転送部123を有しており、ゲートウェイB21は、IKE部211及びIPSec部212を有している。

【0044】そして、IKE部111が、IKE部211と鍵交換を行う（ステップ10）と、これらはそれぞれ、IPSec部112、IPSec部212に鍵設定を行う（ステップ11）。この鍵交換としては、IKEによる従来の鍵交換技術を用いる。そして、鍵設定によって、それぞれのIPSec部に共通の鍵が設定される。

【0045】次に、鍵交換を行ったゲートウェイA111のIKE部111は、鍵転送部113に鍵転送要求を行い（ステップ12）、この鍵転送部113は、ゲートウェイA212の鍵転送部123に鍵転送を行う（ステップ13）。鍵転送を受けた鍵転送部123は、IPSec部122に鍵設定を行う（ステップ14）。

【0046】このようにすることによって、ゲートウェイB21のIPSec部212は、ゲートウェイA111のIPSec部112とIPSec通信を行うことができるとともに、ゲートウェイA111に障害が

発生して、これと通信を行うことができなくなった場合にあっては、ゲートウェイA212のIPSec部122とIPSec通信を行うことが可能となる（ステップ15）。

【0047】次に、図3を用いて、上記鍵転送の処理手順について詳細に説明する。同図は、本実施形態の大規模IPSec VPNシステムにおける鍵転送プロトコルの動作を表わす動作手順図である。まず、ゲートウェイA111の鍵転送部113が、ゲートウェイA212の鍵転送部123に対して、鍵転送を要求する（ステップ20）。

【0048】これに対して、鍵転送部123は、鍵転送部113にOK信号を返す（ステップ21）。このときのOK信号は、IPSec処理の一種である認証付暗号ESP（Encapsulating Security Protocol）により暗号化されて送信される。

【0049】OK信号を受けた鍵転送部113は、このOK信号の認証符号を検査し、鍵を転送する相手が本物のゲートウェイA212であることを確認する（ステップ22）。そして、鍵転送部113は、鍵転送部123に鍵転送を行う（ステップ23）。

【0050】このときの鍵データも認証付暗号ESPによってIPSec処理される。このような暗号化を行うことによって、LAN A10内に悪意のユーザが存在しても、盗聴などを行うことはできない。そして、鍵転送部123は、送信されてきた鍵データの認証符号を検査し、鍵データを送ったのが本物のゲートウェイA111であることを確認する（ステップ24）。

【0051】最後に、鍵転送部123は、転送された鍵を自らの鍵として設定するとともに、鍵転送部113に対して、OK信号を返す（ステップ25）。このOK信号については、特に認証付暗号ESPによるIPSec処理を行う必要はないが、行ってもかまわない。

【0052】次に、第一実施形態の大規模IPSec VPNシステムの処理手順について、図4及び図5を参照して説明する。図4は、本実施形態における鍵交換及び鍵転送を説明するためのものであり、図5は、鍵転送が行われた後に、鍵交換を行った大規模LANにおけるゲートウェイが故障した場合に、どのようにIPSec通信が実現されるのかを説明するためのものである。

【0053】なお、これらの図において、R1、R2、R3は通信回線上に存在し、それぞれゲートウェイB21、ゲートウェイA111、ゲートウェイA212との情報の送受信を中継するルータであり、これら以外の構成及びその機能については、図1と同様である。

【0054】まず、図4において、ゲートウェイA111とゲートウェイB21の間で、鍵交換が行われると（ステップ30）、ゲートウェイA111は、ゲートウェイA212に対して上述したようなネゴシエー

ションを行って、鍵転送を行う(ステップ31)。

【0055】次に、図5において、ゲートウェイA1 11に障害が発生し、通信回線を介した通信が行えなくなると(ステップ40)、ルーティングプロトコルによってR2がこれを認識するとともに、R1、R3にその情報を伝達し、ゲートウェイA1 11宛の全てのパケットを、ゲートウェイA2 12に転送するように、経路情報が修正される(ステップ41)。

【0056】そして、LAN B20におけるホストb (Host b)が、LAN A10におけるホストa (Host a)に対してパケットを発信すると(ステップ42)、ゲートウェイB 21は、このパケットを受け取って、正常時と同様にIPSecのカプセル化を行って(ステップ43)、最寄りのルータR1に転送する。このとき、ステップ41により転送経路情報が変更されているため、通信回線を通ったパケットは、鍵交換を行ったゲートウェイA1 11ではなく、最終的に、ゲートウェイA2 12にたどり着く(ステップ44)。

【0057】ゲートウェイA2 12は、ゲートウェイB 21と共有する鍵をもっているため、これを使って逆カプセル化を行い(ステップ45)、この逆カプセル化されたパケットは、ゲートウェイA2 12によって、ホストaに転送される(ステップ46)。このようにして、ゲートウェイA1 11の障害にも拘わらず、ホストaとホストb間のIPSec通信は成立する。

【0058】[第二実施形態]次に、本発明の第二実施形態につき、図6を参照して説明する。同図は、本実施形態の大規模IPSec VPNシステムの機能を示すブロック図である。本実施形態は、第一実施形態と比較して、LAN A10において、鍵転送が複数回行われる点で相違する。

【0059】同図に示すように、本実施形態の大規模IPSec VPNシステムのLAN A10は、ゲートウェイA1 11、ゲートウェイA2 12、ゲートウェイA3 13を有している。これ以外の構成及びその機能については、図1におけるものと同様である。まず、ゲートウェイA1 11とゲートウェイB 21間で鍵交換が行われると(ステップ50)、ゲートウェイA1 11は、この鍵を自らに設定するとともに、ゲートウェイA2 12に対して鍵転送を行う。

【0060】鍵転送を受けたゲートウェイA2 12は、自ら鍵設定を行うとともに、さらにゲートウェイA3 13に対して、鍵転送を行う。そして、ゲートウェイA3 13は、自ら鍵設定を行うとともに、鍵をさらにゲートウェイA1 11に送信し、ゲートウェイA1 11が、この送信されてきた鍵が、自分が転送した鍵と一致することを確認して鍵転送を終了する(ステップ51)。

【0061】なお、本実施形態においては、LAN A

10内の3台のゲートウェイ間で、鍵転送を行っているが、より多くのゲートウェイ間で同様の処理を行うこともできる。また、本実施形態においては、鍵転送を受けたゲートウェイが、次に他のゲートウェイに鍵転送を順次行う手順としているが、より多くのゲートウェイ間で転送処理を行う場合には、所定の鍵転送経路を設定するなどして、鍵交換を行ったゲートウェイと鍵転送を受けたゲートウェイをコピー元として、まだ鍵転送を受けていないゲートウェイに対し、複数の転送を同時に実行することによって、速やかに転送を行うことも可能である。

【0062】さらに、マルチキャスト(Multicast)IPSecによって、大規模LANのゲートウェイに一齐に鍵転送し、鍵設定を行うようにしてもよい。また、以上の実施形態では、LAN B20において、鍵転送処理を行っていないが、LAN B20が複数のゲートウェイを有する場合にはLAN A10における場合と同様に、必要に応じて鍵転送による鍵の共有化を行うことはもちろん可能である。

【0063】加えて、これらの実施形態におけるゲートウェイの機能を、VPN以外に応用することも可能である。すなわち、このような鍵転送機能による鍵の共有化を、例えば、インターネット上にショップを提供するサーバなどの情報処理装置(鍵共有情報処理装置)に用いることにより、インターネットショッピングにおいてセキュリティを確立した後に、一部の情報処理装置に障害が発生したとしても、通信不能となることを防止することが可能となる。

【0064】そして、このような処理についても、上記実施形態において、ゲートウェイの代わりに鍵共有情報処理装置を用いることにより、同様の構成(ただし、この場合、LAN A10は大規模でなくともよい。)で、同様の鍵転送プロトコルを用いて実現することが可能である。

【0065】大規模IPSec VPNシステムにおける処理手順をこのような順序とすれば、大規模LAN内のゲートウェイが鍵をコピーすることによって、実際には鍵交換をしていない相手とも鍵を共有することができ、複数のゲートウェイを有する大規模なLANとIPSecによるVPNを構築するにあたり、その一部のゲートウェイの障害などによる通信不能を防止することが可能となる。また、大規模LAN内のゲートウェイ間における鍵の共有化を、鍵転送によって行うことにより、このような鍵の共有化を鍵交換によって行う場合に比較すると、装置にかかる負荷を大幅に削減することが可能となる。

【0066】上記の実施形態における鍵転送等は、大規模IPSec VPNプログラムにより実行される。この大規模IPSec VPNプログラムは、コンピュータの各構成要素に指令を送り、所定の処理、例えば、鍵

転送処理等を行わせる。これによって、これらの処理は、大規模IPSec VPNプログラムとコンピュータとが協働したゲートウェイA1 11、ゲートウェイA2 12等により実現される。

【0067】なお、大規模IPSec VPNプログラムは、コンピュータのROMやハードディスクに記憶させる他、コンピュータ読み取り可能な記録媒体、例えば、外部記憶装置及び可搬記録媒体等に格納することができる。外部記憶装置とは、磁気ディスク等の記録媒体を内蔵し、例えばゲートウェイA1 11などに外部接続される記憶増設装置をいう。一方、可搬記録媒体とは、記録媒体駆動装置（ドライブ装置）に装着でき、かつ、持ち運び可能な記録媒体であって、例えば、CD-ROM、フレキシブルディスク、メモ리카ード、光磁気ディスク等をいう。

【0068】そして、記録媒体に記録されたプログラムは、コンピュータのRAMにロードされて、CPUにより実行される。この実行により、上述した本実施形態のゲートウェイA1 11、ゲートウェイA2 12等の機能が実現される。さらに、コンピュータで大規模IPSec VPNプログラムをロードする場合、他のコンピュータで保有された大規模IPSec VPNプログラムを、通信回線を利用して自己の有するRAMや外部記憶装置にダウンロードすることもできる。このダウンロードされた大規模IPSec VPNプログラムも、CPUにより実行され、鍵転送処理等を実現する。

【0069】なお、本発明は以上の実施形態に限定されるものではなく、これをVPN構築以外の場合にも応用することができる。例えば、インターネットショッピングにおいて、利用者端末が、ショップのサーバとセキュリティを確立する際に、ショップの別個のサーバに鍵転送を行うことによって、利用者のショッピング中にショップのサーバに障害が発生しても、その別個のサーバに以降の処理を代行させることによって、通信不能とならなくするなど、適宜設計変更できるものである。

【0070】

【発明の効果】以上のように、本発明によれば、複数のゲートウェイを有する大規模なLANとIPSecによるVPNを構築する場合に、一部のゲートウェイの障害などによる通信不能を防止することができる。

【0071】また、鍵交換によって装置にかかる負荷を大幅に軽減することが可能となる。すなわち、IKEによる鍵交換は、公開鍵暗号技術にもとづく処理であり、他の処理に比べて非常に負荷が大きく、障害時の迂回を考えて2つ以上のゲートウェイとそれぞれ鍵交換を行えば、ゲートウェイの台数分だけ鍵交換を行う必要があるが、本方式では1度の鍵交換でよい。

【0072】さらに、システム全体を安価に構築することが期待できる。これは、パケットがどのゲートウェイ

に渡されるかはインターネット上のルータが決める方式であるため、大規模なLANにアクセスする側のLANは、相手のどのゲートウェイと通信しているかを意識しなくて良いからである。すなわち、これは本方式を実現するためにアクセスする側のゲートウェイに特別な仕掛けが必要ないことを意味する。

【0073】このようなネットワークは、一般に、1つの大規模LANに多数の小規模LANがアクセスする構成をとるため、小規模LAN側のゲートウェイとして、IPSec/IKEに対応した通常のIPSec ゲートウェイを用いることができれば、システム全体として安価なものとなる。

【0074】また、大規模IPSec VPNプログラムは、コンピュータの各構成要素へ所定の指令を送ることにより、このコンピュータに、鍵転送機能等を実現させることができる。これによって、これらの機能等は、大規模IPSec VPNプログラムとコンピュータとが協働したゲートウェイ等により実現可能である。

【図面の簡単な説明】

【図1】本発明の第一実施形態における大規模IPSec VPNシステムの構成を示すブロック図である。

【図2】本発明の第一実施形態における大規模IPSec VPNシステムのゲートウェイの機能を示すブロック図である。

【図3】本発明の各実施形態における大規模IPSec VPNシステムの鍵転送プロトコルの動作を示す動作手順図である。

【図4】本発明の第一実施形態における大規模IPSec VPNシステムの機能を示すブロック図（1）である。

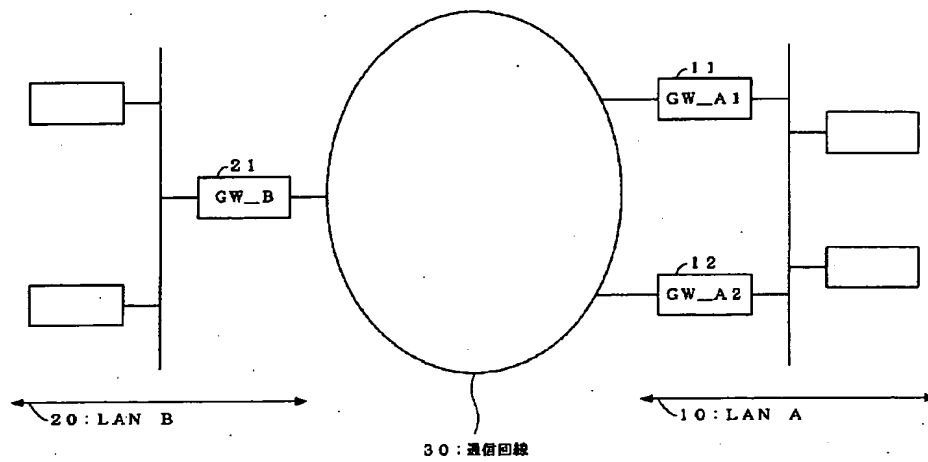
【図5】本発明の第一実施形態における大規模IPSec VPNシステムの機能を示すブロック図（2）である。

【図6】本発明の第二実施形態における大規模IPSec VPNシステムの機能を示すブロック図である。

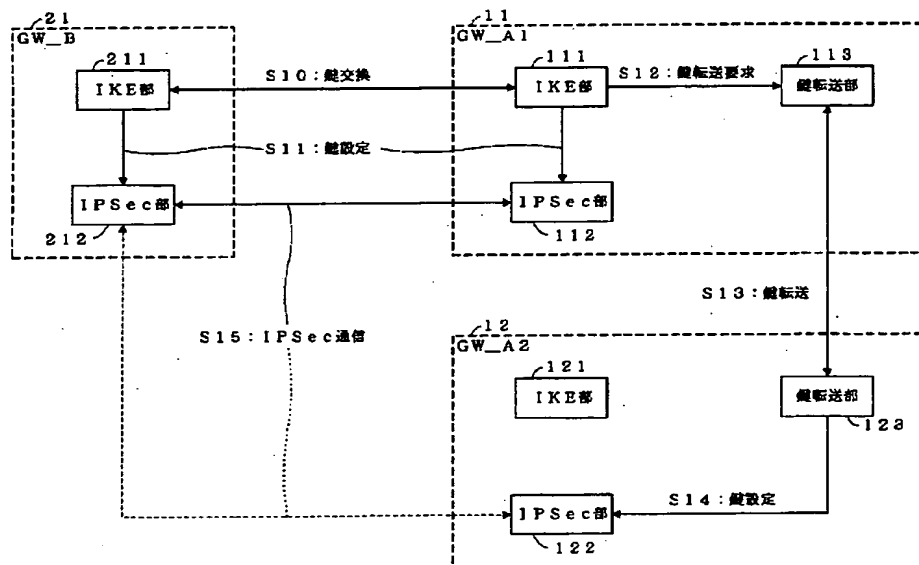
【符号の説明】

- 10 LAN A
- 11 ゲートウェイA1 (GW_A1)
- 12 ゲートウェイA2 (GW_A2)
- 13 ゲートウェイA3 (GW_A3)
- 14 ホスタ (Host a)
- 20 LAN B
- 21 ゲートウェイB (GW_B)
- 22 ホストb (Host b)
- 30 通信回線
- 31 ルータ1 (R1)
- 32 ルータ2 (R2)
- 33 ルータ3 (R3)

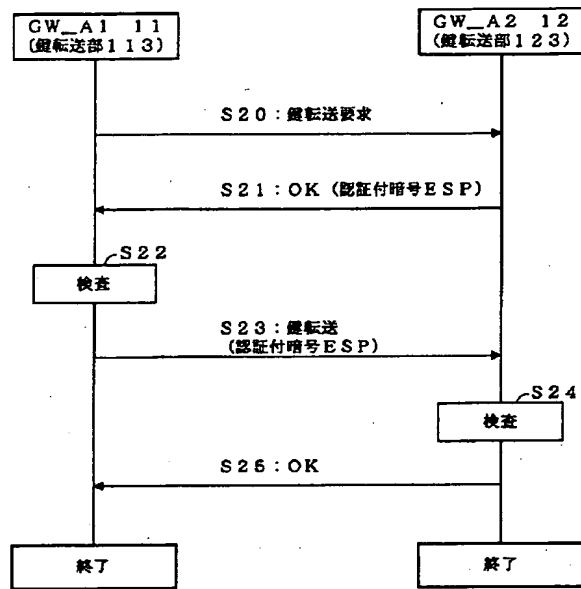
【図1】



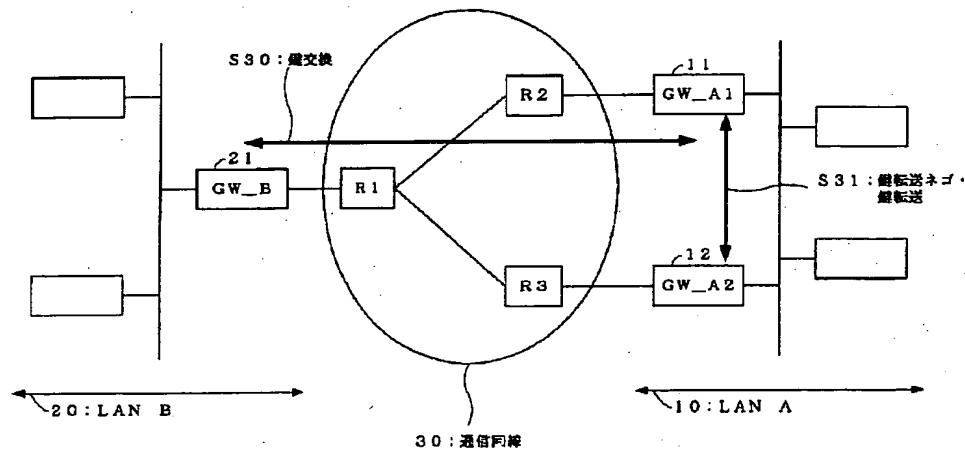
【図2】



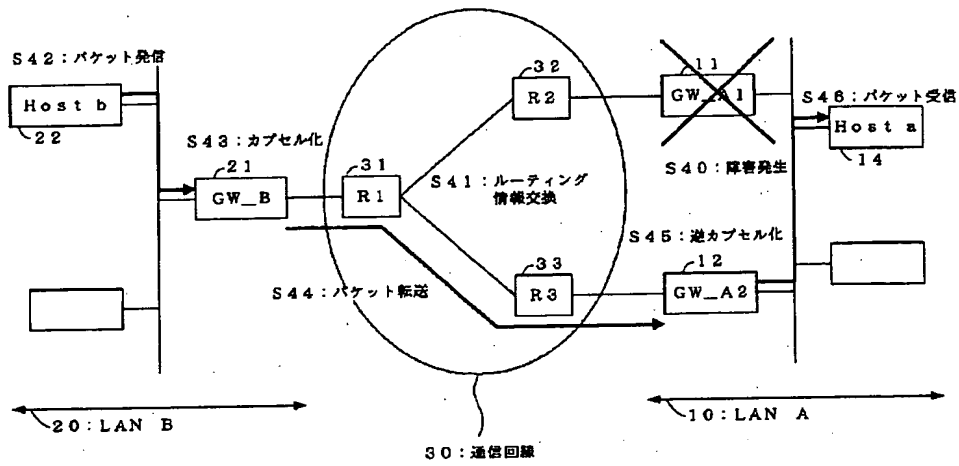
【図3】



【図4】



【図5】



【図6】

